UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal Action
	)	No. 24-cr-10201-PBS
QUENTIN MCDONALD,	)	
Defendant.	)	

MEMORANDUM AND ORDER

January 12, 2026

Saris, J.

INTRODUCTION

A federal grand jury indicted Defendant Quentin McDonald and three codefendants on various counts related to the February 19, 2024, armed robbery of a cash courier in Swansea, Massachusetts. In order to identify suspects, a law enforcement officer obtained search warrants for three cellular service providers to turn over a "tower dump" of records of communications made in the vicinities of the robbery and other related events.

Now before the Court is McDonald's motion to suppress the cell-site location information procured through the execution of the warrants. McDonald argues that tower dumps are Fourth Amendment searches and thus that the warrants were constitutionally required. Neither the Supreme Court nor the First Circuit has addressed the applicability of the Fourth Amendment to tower dumps,

and the case law is unsettled. The government responds that even if the Fourth Amendment requires search warrants for tower dumps, which it disputes, the warrants obtained here were sufficiently particular, and, in the alternative, law enforcement relied on the warrants in good faith.

After hearing, the Court **DENIES** McDonald's motion (Dkt. 142).

BACKGROUND

The following facts are undisputed for purposes of McDonald's motion and are drawn primarily from the "affidavit on which the challenged warrant[s] rest[]." United States v. Jackson, 118 F.4th 447, 449 (1st Cir. 2024).

I. Tower Dumps

Cellular devices communicate primarily by sending and receiving data through nearby cell towers. When a device connects with a cell tower, the tower records various items of information, such as the time of the communication, certain unique identifiers associated with the device, and the source and destination telephone numbers. These data enable law enforcement to obtain cell-site location information ("CSLI"), i.e., the locations of devices based on their interactions with cell towers. See Carpenter v. United States, 585 U.S. 296, 301 (2018).

A "download of information on all the devices that connected to a particular cell [tower] during a particular interval" -- as opposed to the longer-term CSLI of an individual device -- is

called a "tower dump." Id. at 316. Tower dumps generally "are used when law enforcement knows the time and place of the crime but not the identity of the suspects." United States v. Medina, 712 F. Supp. 3d 226, 237 (D.R.I. 2024), vacated on other grounds, 125 F.4th 310 (1st Cir. 2025).

II. The Robbery

At approximately 12:30am on February 19, 2024, surveillance footage captured two individuals enter the parking lot of a U-Haul facility at 403 Bedford Street in Abington, Massachusetts. The individuals were wearing dark sweatshirts and sweatpants. For the next few minutes, the two individuals stood near a key drop box. They then walked to a parked U-Haul van, entered it, and drove off the lot.

Later that morning, at approximately 10:52am, the U-Haul van was captured on video entering the parking lot of Bay Coast Bank at 330 Swansea Mall Drive in Swansea, Massachusetts. The van then drove into an adjacent parking lot from which the bank was visible.

At approximately 12:36pm, a courier carrying over $400,000 in cash collected from local cannabis dispensaries arrived at the bank. The courier removed two bags of cash from the trunk of his vehicle and set them on the ground. Then, at approximately 12:38pm, the U-Haul van reentered the bank's parking lot, pulling up alongside the courier's vehicle. Two men wearing dark sweatshirts and sweatpants exited the U-Haul van and held the courier at

gunpoint before restraining his hands with a zip-tie, pepper-spraying him, and loading the bags of cash into the van. The two men then drove away.

A few minutes later, a witness with a dashboard camera drove down a stretch of Reed Street about a mile away from Bay Coast Bank. Footage from the camera showed a U-Haul van parked on the side of the road. At approximately 12:42pm, a dark Jeep Grand Cherokee pulled up in front of the U-Haul van. Another eyewitness reported observing two men unloading items from the U-Haul van as it began to catch fire. As the U-Haul van became engulfed in flames, the two men boarded the Jeep, which drove away. Law enforcement subsequently recovered a canister of pepper spray from the scene.

III. The Search Warrants

Based on these events, law enforcement believed that the same individuals were involved in the theft of the U-Haul van on Bedford Street, the robbery of the courier on Swansea Mall Drive, and the fire on Reed Street. Law enforcement also believed that the suspects had likely been using cell phones to coordinate the robbery and communicate with the driver of the Jeep.

In an effort to identify the perpetrators, Special Agent Eric Mercer applied for and obtained search warrants seeking tower-dump CSLI from cell towers providing service to the following addresses on February 19, 2024: (1) 403 Bedford Street from 12:15am to

12:45am (i.e., the time the individuals took the van from the U-Haul facility); (2) 330 Swansea Mall Drive from 11:30am through 12:00pm (i.e., the time the individuals awaited the courier in the parking lot adjacent to Bay Coast Bank); (3) 330 Swansea Mall Drive from 12:30pm through 12:45pm (i.e., the time the individuals robbed the courier); and (4) 300 Reed Street from 12:30pm through 1:00pm (i.e., the time the U-Haul van was set on fire). Agent Mercer's warrant application sought the phone numbers, location data, and other identifying information for any communications made in these intervals, but not the contents of the communications themselves. The application limited the records to be seized to only those corresponding with communications made through at least two of the four cell towers in question.

The Magistrate Judge issued the requested search warrants on March 14, 2024. The search authorized by the warrants identified three cellular devices that connected with at least two towers during the relevant time periods. Those three devices belonged to McDonald and two of his codefendants.

DISCUSSION

McDonald moves to suppress the CSLI obtained through the tower dumps. McDonald's argument proceeds in three steps, each of which must be accepted for his motion to succeed. First, he contends that a tower dump is a Fourth Amendment "search" and thus that a warrant is constitutionally required. See Carpenter, 585 U.S. at

316 (leaving this question open). Second, he asserts that the warrants obtained by Agent Mercer failed the Fourth Amendment's particularity requirement. See U.S. Const. amend. IV (requiring warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized" (emphasis added)). Third, he argues that the CSLI obtained through the warrants must be suppressed because the good-faith exception to the exclusionary rule does not apply. See generally United States v. Leon, 468 U.S. 897, 913-25 (1984) (delineating this exception).

As explained below, McDonald has a strong argument at the first step: that a tower dump constitutes a search necessitating a warrant under the Fourth Amendment, absent the applicability of an exception to the warrant requirement. However, McDonald's argument falters at the second and third steps. The warrants obtained by law enforcement were sufficiently particular and, even if they were not, the good-faith exception would preclude suppression.

I. Warrant Requirement

The threshold question raised by McDonald is whether a tower dump is a Fourth Amendment search. The Court concludes that it is.

The Fourth Amendment guards against "unreasonable searches and seizures." U.S. Const. amend. IV. This constitutional guarantee "protects people, not places." Katz v. United States, 389 U.S. 347, 351 (1967). As relevant here, if a person "'seeks to

preserve something as private[]' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,'" a Fourth Amendment "search" occurs when the government intrudes upon that "private sphere." Carpenter, 585 U.S. at 304 (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

In Carpenter, the Supreme Court held that individuals have reasonable expectations of privacy in their long-term CSLI, such that the government's "accessing seven days of CSLI constitutes a Fourth Amendment search." Id. at 310 n.3. "[T]he intersection of two lines of cases" informed the Court's holding. Id. at 306. First, the Court examined cases involving "a person's expectation of privacy in his physical location and movements." Id. The Court explained that tracking an individual's location through "detailed, encyclopedic, and effortlessly compiled" CSLI impinges on this reasonable expectation. Id. at 309. Second, the Court distinguished cases applying the third-party doctrine, under which the "voluntary exposure" of information may vitiate reasonable expectations of privacy. Id. at 315. The Court "decline[d] to extend" this doctrine "to the collection of CSLI" due to CSLI's "unique nature," noting that individuals have "no way to avoid leaving behind a trail of" CSLI apart from the impractical option of "disconnecting [a] phone from the network." Id.

After Carpenter, district courts have split on whether tower dumps involving short-term CSLI are subject to the Fourth

Amendment -- a question that the Supreme Court expressly declined to address, see id. at 316. Some district courts have extended Carpenter's reasoning to tower dumps and thus held that they constitute Fourth Amendment searches. See United States v. Spurlock, 778 F. Supp. 3d 1136, 1142-45 (D. Nev. 2025); In re Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers, No. 25-CR-38, 2025 WL 603000, at *2-6 (S.D. Miss. Feb. 21, 2025); Medina, 712 F. Supp. 3d at 236-46. Others have held the opposite. See United States v. Dickerson, No. 24-CR-83, 2025 WL 2960141, at *9-11 (E.D. Wis. June 10, 2025), report and recommendation adopted, 2025 WL 2779095 (E.D. Wis. Sep. 30, 2025); United States v. Pricop, 775 F. Supp. 3d 1036, 1038-39 (D. Ariz. 2025); United States v. Williams, 741 F. Supp. 3d 642, 650-51 (E.D. Mich. 2024); United States v. Matthews, No. 22-CR-429, 2024 WL 688666, at *3-4 (N.D. Ga. Feb. 20, 2024); United States v. Walker, No. 18-CR-37, 2020 WL 4065980, at *6-8 (E.D.N.C. July 20, 2020); United States v. Rhodes, No. 19-CR-0073, 2020 WL 9461131, at *2-3 (N.D. Ga. June 18, 2020), report and recommendation adopted, 2021 WL 1541050 (N.D. Ga. Apr. 20, 2021).

No circuit court of appeals has decided the issue. The Seventh Circuit has rejected a defendant's contention that Carpenter resolved the question but has not squarely held that tower dumps do not constitute Fourth Amendment searches. See United States v. Adkinson, 916 F.3d 605, 610-11 (7th Cir. 2019) (per curiam).

Similarly, the Eighth Circuit has declined to resolve the question. See United States v. James, 3 F.4th 1102, 1106 n.3 (8th Cir. 2021). The Fifth Circuit and certain judges of the Fourth Circuit have espoused competing views with respect to geofencing, a similar but distinct technology from tower dumps. Compare United States v. Smith, 110 F.4th 817, 830-36 (5th Cir. 2024) (holding that geofencing constitutes a Fourth Amendment search), cert. denied, No. 24-7237, 2025 WL 3131804 (U.S. Nov. 10, 2025), with United States v. Chatrie, 136 F.4th 100 (4th Cir. 2025) (affirming district court judgment in geofencing case with no controlling opinion), petition for cert. filed, No. 25-112 (U.S. July 28, 2025).

The issue is a close call. This Court concludes that the courts that have held that tower dumps constitute a Fourth Amendment search have the stronger argument. The Court finds Medina's in-depth discussion of this issue persuasive, see 712 F. Supp. 3d at 236-46, and briefly highlights the two primary bases for the conclusion that search warrants are required to execute tower dumps.

First, although tower dumps typically seek CSLI over a shorter duration of time than the longer-term individual CSLI at issue in Carpenter, the same privacy interests are implicated. Tower dumps seek "time-stamped data [that] provides an intimate window into a person's life, revealing not only his particular movements, but

through them his 'familial, political, professional, religious, and sexual associations.'" Carpenter, 585 U.S. at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). For example, even though the tower dumps here were executed to identify individuals operating primarily on "public thoroughfares" to commit a crime, they may have also incidentally collected data regarding those individuals' activities in "private residences, doctor's offices, political headquarters, and other potentially revealing locales." Id. And tower dumps, like searches of individualized CSLI, allow law enforcement to "travel back in time to retrace a person's whereabouts," even if the identity of that person is not yet known. Id. at 312; see id. at 315 (noting that CSLI provides a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years"). Critically, regardless of whether the government seeks longer-term individual CSLI or shorter-term tower-dump CSLI, the location data at issue is "detailed, encyclopedic, and effortlessly compiled," thus implicating the privacy interests of the countless people who "carry cell phones with them all the time." Id. at 309, 311.

Second, Carpenter's rationale for declining to apply the third-party doctrine to long-term individual CSLI applies with equal force to tower dumps. Carpenter "recognize[d] that CSLI is an entirely different species of business record" from those usually underpinning the third-party doctrine, such that the fact

that CSLI is shared with wireless carriers does not undermine the privacy interests at issue. Id. at 318. And as the Supreme Court noted, "[v]irtually any activity on [a] phone generates CSLI," effectively forcing individuals to "leav[e] behind a trail of location data." Id. at 315. For that reason, and because a cell phone is "almost a 'feature of human anatomy,'" id. at 311 (quoting Riley v. California, 573 U.S. 373, 385 (2014)), users of cell phones cannot reasonably be viewed as voluntarily exposing their location information. These principles are inherent to the "unique nature" of CSLI, id. at 309, whether it is collected through an individualized search or through a tower dump.

II. Particularity

The government points out that even if the Fourth Amendment requires a search warrant for a tower dump, law enforcement in this case did obtain warrants. McDonald does not dispute that sufficient probable cause existed for law enforcement to obtain the warrants. Rather, he contends that the warrants were insufficiently particular in describing the places to be searched and the items to be seized. The Court disagrees.

A search warrant complies with the Fourth Amendment only if it "particularly describ[es] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This particularity requirement, which "exists 'to prevent wide-ranging general searches by the police,'" "implicat[es] two distinct

demands." United States v. Corleto, 56 F.4th 169, 176 (1st Cir. 2022) (quoting United States v. Moss, 936 F.3d 52, 58 (1st Cir. 2019)). First, the warrant "must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize." Id. (quoting United States v. Lindsey, 3 F.4th 32, 40 (1st Cir. 2021)). Second, the warrant "cannot be too broad in the sense that it includes items that should not be seized." Id. (quoting Lindsey, 3 F.4th at 40).

The warrants obtained by the special agent satisfy both of these conditions. First, the warrants provided sufficient information delineating the government's search and seizure. Attachment A to the warrant application identified the four cell towers and specific time periods to be searched, and Attachment B listed six categories of data to be seized, including telephone numbers, unique device identifiers, communication metadata, and location information, while specifically excluding the contents of communications. These descriptions "provided sufficient guidance to 'control the [government]'s judgment in selecting what to take.'" Lindsey, 3 F.4th at 41 (quoting United States v. Tiem Trinh, 665 F.3d 1, 15 (1st Cir. 2011)).

Second, the warrants were narrowed in several important ways to avoid an overbroad seizure. Most importantly, the warrants were tailored "both geographically and temporally" to the events at issue (i.e., the theft of the U-Haul van, the van's waiting for

the courier's arrival, the robbery of the courier, and the van's being set on fire). James, 3 F.4th at 1106. Each tower dump was geographically associated with one of these four events and was limited to an interval of no more than thirty minutes, corresponding to the times at which video footage and eyewitnesses had shown that the event had occurred. See id. (holding that warrants for tower dumps satisfied particularity requirement where "they covered only the cellular towers near each robbery" and were confined to approximately ninety-minute time periods). Further, the warrants allowed law enforcement to seize only the CSLI of devices that connected to two or more of the four cell towers in question, thereby ruling out individuals who may have been incidentally present near only one of the events. And the warrants did not seek the contents of any communications, only the identifying information associated with them.

The Court is unpersuaded by McDonald's argument that the warrants were "general warrants" lacking in particularity. General warrants historically "specified only an offense," leaving "to the discretion of the executing officials the decision as to . . . which places should be searched." United States v. Levin, 874 F.3d 316, 323 (1st Cir. 2017) (quoting Steagald v. United States, 451 U.S. 204, 220 (1981)); see also Riley, 573 U.S. at 403 (noting that colonial-era general warrants "allowed British officers to rummage through homes in an unrestrained search for evidence of

criminal activity"). The warrants at issue here, in contrast, specifically identify the four cell towers to be searched, while limiting the seized information according to the above-described parameters. The warrants thus demarcated "about the narrowest definable search and seizure reasonably likely to obtain" the identities of the perpetrators. Corleto, 56 F.3d at 177 (quoting United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)).

III. Good-Faith Exception

Finally, in the alternative, the Court concludes that even if the warrants here were not sufficiently particular, the good-faith exception to the exclusionary rule would prevent suppression of the evidence derived from the warrants. McDonald's argument thus falls short at the third step as well as the second.

Although the Fourth Amendment "says nothing about suppressing evidence obtained in violation of [its] command," the judicially created "exclusionary rule" allows for suppression in some instances. Davis v. United States, 564 U.S. 229, 236 (2011). The exclusionary rule is prophylactic: its "sole purpose . . . is to deter future Fourth Amendment violations." Id. at 236-37. For that reason, courts only apply the exclusionary rule where "the deterrence benefits of suppression . . . outweigh its heavy costs." Id. at 237.

In evaluating the deterrence benefits of applying the exclusionary rule, courts must gauge "'the culpability of the law

enforcement conduct' at issue." Id. at 238 (quoting Herring v. United States, 555 U.S. 135, 143 (2009)). Exclusion is generally justified where "police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights," but not when "police act with an objectively 'reasonable good-faith belief' that their conduct is lawful." Id. (first quoting Herring, 555 U.S. at 144; and then quoting Leon, 468 U.S. at 909). In other words, an exception to the exclusionary rule exists when officers act in good faith or even where "their conduct involves only simple, 'isolated' negligence." Id. (quoting Herring, 555 U.S. at 137).

As relevant here, the good-faith exception can apply where an officer has acted "in objectively reasonable reliance on a subsequently invalidated search warrant." Leon, 468 U.S. at 922. "The existence of a warrant issued by a magistrate will usually establish this form of good faith," unless one of four circumstances applies:

> (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) where the issuing magistrate wholly abandoned his judicial role; (3) when an affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) when, depending on the circumstances of the particular case, a warrant is so facially deficient -- i.e., in failing to particularize the place to be searched or the things to be seized -- that the executing officers cannot reasonably presume it to be valid.

United States v. Bain, 874 F.3d 1, 21 (1st Cir. 2017) (cleaned up) (quoting Leon, 468 U.S. at 923).

McDonald does not argue that the Magistrate Judge was "misled" or "wholly abandoned his judicial role" in issuing the warrants, or that the special agent's application was "so lacking in indicia of probable cause" that no reasonable officer could have believed probable cause existed. Id. (quoting Leon, 468 U.S. at 923). Rather, only the fourth circumstance is relevant here: McDonald argues that the tower dump warrants issued by the Magistrate Judge were "facially deficient . . . in failing to particularize the place to be searched or the things to be seized." Id. (quoting Leon, 468 U.S. at 923).

The Court disagrees. For the reasons explained above, the warrants obtained by law enforcement here satisfied the Fourth Amendment's particularity requirement. And even if they did not, they certainly were not "so facially deficient" that executing officers could not "reasonably presume [them] to be valid." Id. (quoting Leon, 468 U.S. at 923). In other words, "regardless of whether the warrant[s] w[ere] sufficiently particular," law enforcement officials "reasonably relied on the warrant[s] when executing their search." Jackson, 118 F.4th at 449. Further, as previously discussed, the warrants were not akin to "general warrant[s]" and thus were not "so obviously lacking in particularity that the [government's] reliance on [them] amounted

to bad faith." Levin, 874 F.3d at 322. Given these circumstances, "the deterrence rationale" of the exclusionary rule "loses much of its force, and exclusion cannot pay its way." Id. (quoting Davis, 564 U.S. at 238). Suppression is not warranted.

ORDER

For the foregoing reasons, McDonald's motion to suppress (Dkt. 142) is **DENIED**.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge